

CONDITIONAL ACCESS SYSTEM FOR SET-TOP BOXESField of the Invention

5 This invention concerns a system for providing conditional access (i.e., managing access) to a device, such as a "consumer electronic device". Examples of such consumer electronic devices include separate devices or "boxes" that may be located on top of, and coupled to a television receiver, i.e., set-top boxes.

10

Background of the Invention

In general, conditional access involves limiting or controlling the communication with a device based on predetermined criteria. Conditional access may be achieved by connecting two devices together when communication therebetween is desired and by disconnecting the two devices from one another when such communication is no longer desired. However, in the context of today's sophisticated computer networks interconnected to form what is known as the world-wide web ("web"), many, if not all, of the devices designed to communicate with the web are "permanently" connected to the web through modem hookups or other means. That is, the devices usually remain physically connected to the web. Typically, access to the web is via a specially designed software package loaded onto a computer and a modem; this software enables a user to connect to an internet service provider who acts as the gate keeper to the web. The user typically pays a monthly fee to the service provider for access to the internet, either on a limited or unlimited basis. The proliferation of users who regularly access the

web as a source of information or even as a means of communicating via E-Mail for both business and personal reasons has created a very competitive market for both service providers and the manufacturers of the necessary hardware. Thus, as one would expect there are numerous service providers, each requiring specialized software for access.

An outgrowth of today's emerging digital consumer electronic products is an opportunity to access the Internet from a user's television. Such access has been accomplished by utilizing the user's television as a monitor or display device in conjunction with a set-top box that provides the software (e.g., a web browser) and hardware (e.g., modem, ethernet, ADSL or any equivalent connection means) needed to interface to the web. For example, the RCA Network Computer manufactured by Thomson Consumer Electronics is such a set-top box that may be connected to both a television and a phone line or the like thereby permitting the user to access the web. Set-top boxes may provide a means for a variety of internet applications (e.g., electronic commerce) from the home, the office or any location without utilizing a personal computer or any general purpose computing device. These set-top boxes have open hardware architectures which would permit easy adaptation of the set-top box thereby permitting use with any of a plurality of service providers.

25

Summary of the Invention

The manufacturers of these set-top boxes may desire that the box only be used with selected service providers. For example, the manufacturer of the box may be compensated by the service provider

for each connection to the service from the box. Thus, the flexibility of the set-top box's open hardware architecture in combination with a competitive market for such devices necessitates the need to provide a system for providing conditional access in the set-top box so that
5 the box can only connect to selected service providers. This invention resides, in part, in recognition of the described problem and, in part, in providing a solution to the problem.

Generally, the present invention defines a method for
10 managing access to a device by sending a first message to a second device; receiving a digital certificate encrypted using a first private key; receiving the first message encrypted using a second private key; authenticating the second device; and establishing a communication channel between the devices.

15 In accordance with one aspect of the present invention, the first message comprises data associated with the first device and a date and time stamp, and the digital certificate comprises data associated with the second device and a second public key.

20 In accordance with another aspect of the present invention, the step of authenticating comprises decrypting the digital certificate using a first public key; decrypting the first encrypted message using the second public key to generate a first decrypted
25 message; and comparing the first decrypted message to the first message.

In accordance with another aspect of the present invention, the method further comprises providing confirmation of

the authentication to said second device by encrypting the first message using the second public key to generate a second encrypted message; and sending the second encrypted message to the second device.

5

In accordance with still another aspect of the present invention, the digital certificate, the first public and first private keys are issued by an independent certificate authority and are associated with the second device.

10

In accordance with yet another aspect of the present invention, a system for managing access between a service provider and a set-top box having a smart card coupled thereto, the set-top box sends a first message to the smart card; receives a smart card (first) digital certificate encrypted using a private key; authenticates the smart card; contacts the service provider and sends a second message to the service provider; receives a service provider (second) digital certificate encrypted using another private key; receives the second message encrypted using yet another private key;

15

authenticates the service provider; provides confirmation to the service provider; and establishes a communication channel with the service provider. Particularly, the two messages contain at least set-top box identification data.

20

In accordance with yet another aspect of the present invention, the smart card includes service provider identification data associated with a plurality of service providers.

25

These and other aspects of the invention will be explained with reference to a preferred embodiment of the invention shown in the accompanying Drawings.

5

Brief Description of the Drawings

Figure 1 is a block diagram of an exemplary implementation of a system for managing access to a device in accordance with the invention; and

10

Figure 2 is a flowchart diagram of an exemplary implementation of the conditional access system of Figure 1.

Figure 3 is a block diagram of an exemplary implementation of the system of Figure 1 wherein any one of a plurality of set-top boxes may communicate with any one of a plurality of service providers.

15

Detailed Description of the Drawings

20

The present invention provides a conditional access system which may be utilized to obtain services from one of a plurality of sources. When implemented within a set-top box, the conditional access system permits the set-top box to authenticate the service provider and/or a smart card used to access services before a communication channel is established. Such a conditional access system may act as a toll bridge for access to services, thereby permitting a mechanism for the manufacturer of the set-top box to collect fees based on use of its set-top box.

25

In Figure 1, the system 10 for managing access to a set-top box (STB) 20, for example, the RCA Network Computer, is depicted. Smart Card (SC) 30 is inserted into or coupled to a smart card reader (not shown) included in STB 20; an internal bus 25 interconnects STB 20 and SC 30 thereby permitting the transfer of data therebetween. Alternately, the functionality of the smart card may be embedded within the set-top box. STB 20 is connected to service provider (SP) 40 via a dial-up link or a direct link, which is depicted as element 45. Certificate Authority (CA) 50 is not directly connected to either SP 40 or STB 20 but issues digital certificates and public and private key pairs, which are used as explained below. These digital certificates are used by service providers and smart card manufacturers. It is within the scope of this invention that the digital certificates could be provided via an on-line connection. Further, it is within the scope of this invention that the role of Certificate Authority may be performed by SP 40 in collaboration with the manufacturer of the STB 20. The conditional access system of the present invention will be described in relation to system 10 as shown in Figure 1 and the flowchart diagram of Figure 2.

This conditional access system is based on authentication of each device (for example, SC 30 and SP 40) communicating with STB 20 prior to establishing a communication channel between a STB 20 and SP 40. Particularly, this conditional access system utilizes an asymmetric key system (i.e., public-key system), wherein only public keys are stored in the set-top box. That is, the set-top box does not store or contain any secrets (i.e., private keys). The foundation of public-key cryptography is the use of two related keys, one public

and one private; the private key being computationally unfeasible of being deduced from the public key which is publicly available.

Anyone with a public key can encrypt a message but only the person or device having the associated and predetermined private key can
5 decrypt it. Similarly, a message can be encrypted by a private key and anyone with access to the public key can decrypt that message. Encrypting messages using a private key may be referred to as "signing" because anyone holding the public key can verify that the message was sent by the party having the private key. This may be
10 thought of as being analogous to verifying a signature on a document.

A digital certificate or certificate is a message sent in the clear (i.e., unencrypted) having a CA 50 signature attached thereto; thus the recipient of the certificate can verify the source or origin of
15 the certificate. These digital certificates are in fact "signed messages" because the signature attached to the message is produced by encrypting either the message itself or a digest of the message (which is obtained by hashing the message, as described later). Unilateral authentication of each device connected to the set-top box is achieved
20 by passing such certificates between the devices and verifying these certificates. Certificate verification involves checking the signature by decryption. These certificates may contain information used by the device receiving the certificate. This information may be related to a device not involved in the passing of this certificate, e.g.
25 information contained in the first digital certificate is related to the service provider as described below. Further, the certificates may contain information associated with the device passing the certificate and a public key of the passing device.

As described above, only public keys are stored in a memory device contained in STB 20. Further, the first and second digital certificates, which may be issued by CA 50, are stored in SC 30 and SP 40, respectively.

5

The following nomenclature will be utilized in the below description of the present conditional access system.

	KCApri1	Private key used to create SC's certificate
10	KCApub1	Public key used to verify SC's certificate
	KCApri2	Private key used to create SP's certificate
	KCApub2	Public key used to verify SP's certificate
	 KSPpub	 SP's Public key
15	KSPpri	SP's Private key

These are used and discussed with respect to authenticating a device such as the smart card or the service provider.

20 After STB 20 is activated and SC 30 is inserted into STB 20, STB 20 sends a first message to SC 30 (see Figure 2, Step 100). This first message contains identification data corresponding to STB 20, for example, such identification data may include the manufacturer's identification data (MID). In response to the first
25 message, SC 30 replies by sending a first digital certificate back to STB 20 (see Figure 2, Step 120). The first digital certificate (i.e., SC's certificate) includes data sent in the clear and an attached signature which is encrypted using KCApri1, the private key which is used to create certificates sent by SC 30. This data may include identification

data corresponding to a selected service provider having a pre-existing agreement with the manufacturer of STB 20. Particularly, this data may also include, in addition to the service provider identification data, a phone number for the service provider which
5 will be used for contacting the service provider as described below.

If SC 30 does not have a digital certificate associated with a service provider (see Figure 2, Step 110), STB 20 may contact an independent party (not shown), download an appropriate digital
10 certificates from the independent party (see Figure 2, Step 114) and transfer them to SC 30 (see Figure 2, Step 116). STB 20 may contact the independent party utilizing an integrated modem. If the digital certificates are downloaded from the independent party, the above process may continue starting at the point where SC 30 replies to the
15 first message by sending a first digital certificate back to STB 20.

Now, STB 20 must authenticate (see Figure 2, Step 130) SC 30 by verifying that SC 30 has passed a valid certificate to STB 20, this involves decrypting the first digital certificate in STB 20 using
20 KCApub1. KCApub1, which is stored in STB 20, is the corresponding public key also assigned by CA 50. After SC 30 is authenticated, the service provider identification data included in the first digital certificate is used by STB 20 to contact the desired service provider, for example SP 40.

25

SC 30 may have more than one digital certificate, each one of which may identify a different service provider. If this is the case, the user may be prompted to select one of the service providers having a valid certificate (see Figure 2, Step 140). Further, if a

service provider has more than one access number, the set-top box may select an alternate number if, for example, the primary number is busy.

5 STB 20 sends a second message to SP 40 (see Figure 2, Step 150); this second message contains similar identification data corresponding to STB 20. For example, such identification data now may include the manufacturer's identification data (MID) and a date and time stamp (DTS). DTS may be downloaded from an electronic
10 program guide or from a special time server or possible through an internal means. In response to the second message, SP 40 replies by sending (1) a second digital certificate (i.e., SP's certificate) and (2) the second message encrypted using KSPpri back to STB 20 (see Figure 2, Step 160). The second digital certificate includes data sent
15 in the clear and an attached signature which is created using KCApri2. This data may include identification data corresponding to the service provider, the validity period (VP) for the second digital certificate and the public key for SP 40, i.e., KSPpub. The identification data may also further include data associated with CA 50 which may be
20 utilized, if necessary, for authentication of SP 40. Now SP 40 must be authenticated; such authentication is achieved utilizing the second digital certificate and the encrypted second message (see Figure 2, Step 170).

25 Particularly, authentication of the service provider involves (1) decrypting the second digital certificate in STB 20 using KCApub2, which is stored therein, (2) decrypting the encrypted second message using the public key of SP 40 (i.e., KSPpub) which is included in the second digital certificate and (3) comparing the

decrypted "encrypted second message" to the original second message sent to SP 40. This ensures that the certificate was received from the desired service provider and not from another source.

5 Further, the data contained in the second digital certificate may be subjected to a one-way hashing algorithm, such as MD5 developed by Ron Rivest or SHA-1 developed by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) prior to being encrypted by KCApri2. If this is
10 the case, authentication may also include hashing the data sent in the clear using the same one-way hashing algorithm and comparing this data to the decrypted data. Similarly, the creation of the first digital certificate may involve the use of such a one-way hashing algorithm.

15 After SP 40 has been authenticated by STB 20, STB 20 sends confirmation of this authentication back to SP 40 (see Figure 2, Step 180). This confirmation involves sending the second message now being encrypted using the public key of SP 40, i.e., KSPpub, back to SP 40. SP 40 can decrypt this message using its associated private
20 key, KSPpri. Finally, STB 20 establishes a communication channel (see Figure 2, Step 190) between STB 20 and SP 40 wherein all future communication may be handled utilizing public-key cryptography and the public and private key pairs associated with SP 40 (i.e. KSPpub and KSPpri).

25

The present invention has been described in terms of an exemplary embodiment in which a single smart card cooperates with a single set-top box to manage access to a single service provider. However, it is within the scope of this invention to provide a

conditional access system which may be extended to permit the smart card to "roam" across (i.e., provide conditional access between) multiple service providers and multiple manufacturers of the set-top boxes. This is particularly illustrated in Figure 3 where SC 30a may be used in any one of STBs 20a, 20b or 20c to access any one of SPs 40a, 40b or 40c. In such a system, each set-top box manufacturer will have a unique MID. The smart card will have a unique first digital certificate for each service provider and for each manufacturer having a predetermined agreement with the service provider. Each set-top box will have unique sets of public keys for verifying these digital certificates. For example, if there are "m" service providers and "n" manufacturers of set-top boxes then the smart card may contain up to "m times n" number of digital certificates.

While the invention has been described in detail with respect to numerous embodiments thereof, it will be apparent that upon a reading and understanding of the foregoing, numerous alterations to the described embodiment will occur to those skilled in the art and it is intended to include such alterations within the scope of the appended claims. Further, it is within the scope of the present invention that the conditional access system defined herein is fully capable of being utilized between any two devices interconnected.